

ABSTRACT OF THE DISCLOSURE

An authentication system providing a safety authentication process of electronic values with the use of mobile terminals which do not have a tamper-resistant function. The electronic value including encrypted value authentication information (F(VPW)), wherein an authentication information (VPW) corresponding to an electronic value specified by a user is acquired by the hash calculation, is stored in user's mobile terminal. In the user authentication process; authentication apparatus generates a random number R and transmits it to mobile terminal, mobile terminal generates value authentication information (F(VPW')) from authentication information (VPW') corresponding to electronic value input by user, further executes a hash calculation on data wherein value authentication information (F(VPW')) and the random number R are concatenated, generates authentication information (F(VPW')||R), transmits it to the authentication apparatus with the electronic value, authentication apparatus decrypts the received electronic value, extracts the value authentication information (F(VPW)) from the electronic value, executes the hash calculation on data wherein value authentication information (F(VPW)) and the random number R are concatenated, generates the authentication information (F(VPW)||R), and collates the received authentication information (F(VPW')||R) with the authentication information (F(VPW)||R), so that the user is authenticated.